METHOD FOR DETECTING ILLEGAL MODIFICATIONS MADE TO MANUFACTURER
SOFTWARE
Application No. 10/583,356
Inventor: Marie-Francoise ERNY
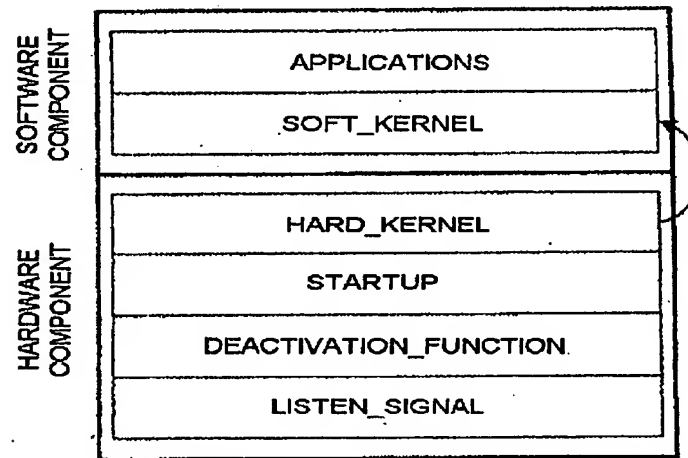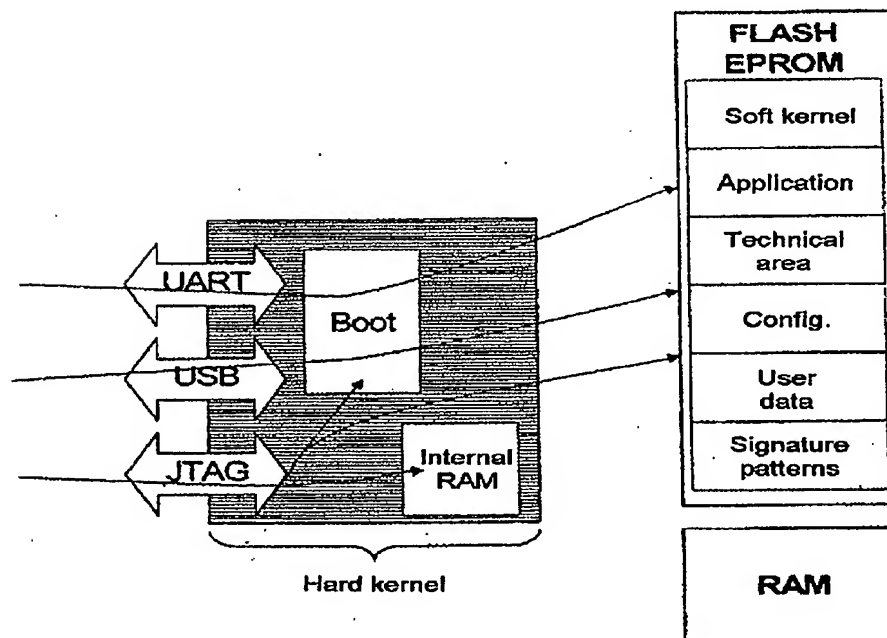*Replacement Sheet*

1/3

FIG.1

FIG. 2

METHOD FOR DETECTING ILLEGAL MODIFICATIONS MADE TO MANUFACTURER
SOFTWARE
Application No. 10/583,356
Inventor: Marie-Francoise ERNY
Replacement Sheet

2/3

FIG.3

1/ Generator of dynamic data (clock, pseudo-random)

2/ Dispatch of DYN

3/ MSG_1 = SHA (DYN received) XOR (*Question*)

5/ *Question received* = SHA (DYN) XOR (MSG_1)

4/ Dispatch of MSG_1

6/ Verification of the semantics of the question received

7/ MSG_2 = SHA (*Question received, DYN*) XOR Key

8/ Dispatch of MSG_2

9/ ANSWER = MSG_2 XOR SHA (*Question, DYN received*)

FIG.5

METHOD FOR DETECTING ILLEGAL MODIFICATIONS MADE TO MANUFACTURER
SOFTWARE
Application No. 10/583,356
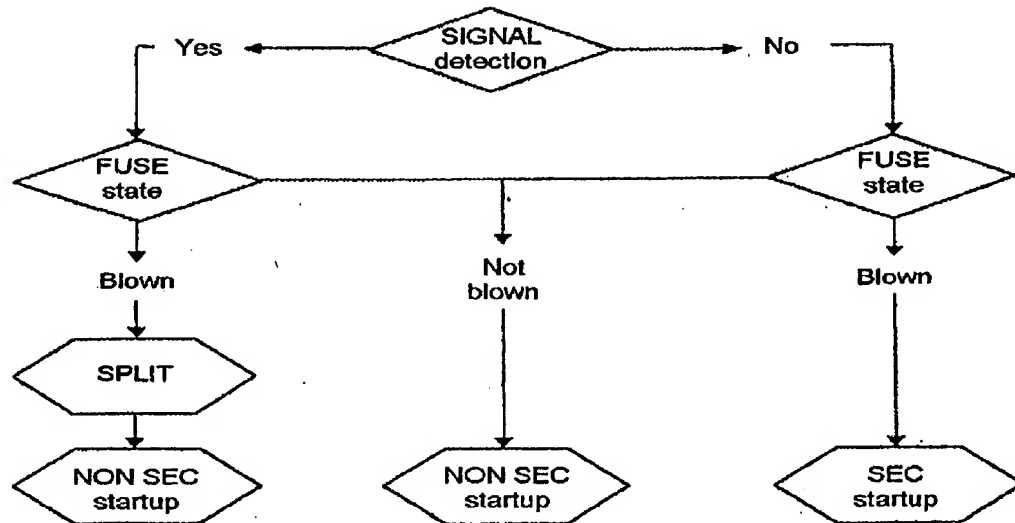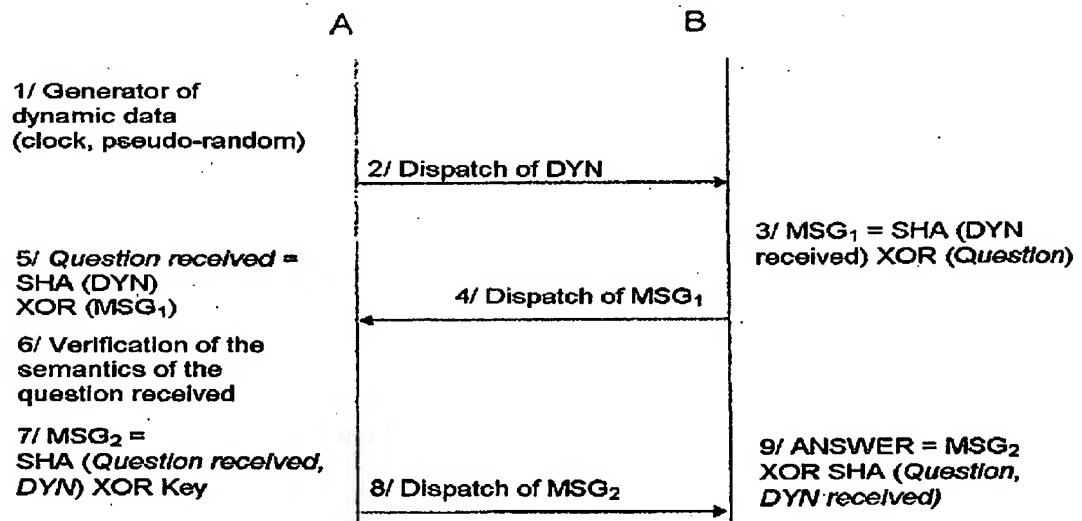Inventor: Marie-Francoise ERNY
Replacement Sheet

3/3

FIG.4